Cryptography Over Elliptic Curve Of The Ring $\mathbb{F}_q[\epsilon], \epsilon^4 = 0$  

CHILLALI ABDELAHIM  
FST DE FEZ  
Department of Mathematics  
FEZ  
MOROCCO  
chil2015@yahoo.fr

Abstract—Groups where the discrete logarithm problem (DLP) is believed to be intractable have proved to be inestimable building blocks for cryptographic applications. They are at the heart of numerous protocols such as key agreements, public-key cryptosystems, digital signatures, identification schemes, publicly verifiable secret sharings, hash functions and bit commitments. The search for new groups with intractable DLP is therefore of great importance. The goal of this article is to study elliptic curves over the ring $\mathbb{F}_q[\epsilon]$, with $\mathbb{F}_q$ a finite field of order $q$ and with the relation $\epsilon^n = 0$, $n \geq 3$. The motivation for this work came from the observation that several practical discrete logarithm-based cryptosystems, such as ElGamal, The motivation for this work came from the observation that several practical discrete logarithm-based cryptosystems, such as ElGamal, Digital Signatures with Hash Functions (DSS) and Public Key Cryptosystems (PKC), are based on the fact that the Discrete Logarithm Problem (DLP) is believed to be intractable.

The following result

\[ \sum_{i=0}^{n-1} a_i \epsilon^i \]

is in the maximal ideal of $A$, where $a_i$ are integers.

Remark 4: Let $Y = \sum_{i=0}^{n-1} Y_i \epsilon^i$ be the inverse of the element $X = \sum_{i=0}^{n-1} X_i \epsilon^i$. Then

\[
\begin{aligned}
Y_0 &= X_0^{-1} \\
Y_j &= -X_0^{-1} \sum_{i=0}^{j-1} Y_i X_{j-i}, \quad \forall j > 0
\end{aligned}
\]

II. ELLIPTIC CURVE OVER A

In this section we suppose $n = 4$. An elliptic curve over ring $A$ is curve that is given by such Weierstrass equation:

\[ Y^2 Z = X^3 + aXZ^2 + bZ^3 \]

where $a, b \in A$ and $4a^3 + 27b^2$ is invertible in $A$. We denote by $E_{a,b}$ the elliptic curve over $A$. The set $E_{a,b}$ together with a special point $O$ -called the point infinity-, a commutative binary operation denoted by $+$. It is well known that the binary operation $+$ endows the set $E_{a,b}$ with an abelian group with $O$ as identity element.

Defining the curve over $A$ with characteristic 2 or 3 is possible, but it is indifferent for our purposes.

Lemma 5: The mapping

\[ \pi_{a,b} : \mathbb{F}_q \to \mathbb{F}_q \]

is a surjective homomorphism of groups.

Proof 6: Consider $[X_1 : Y_1 : Z_1]$ and $[X_2 : Y_2 : Z_2]$ in $E_{a,b}$. We have

\[ (1) : \pi_{a,b}([X_1 : Y_1 : Z_1] + [X_2 : Y_2 : Z_2]) = \pi_{a,b}([X_1 : Y_1 : Z_1]) + \pi_{a,b}([X_2 : Y_2 : Z_2]). \]

We now quickly show how one can also obtain results (1) using maple procedure "some and proj2". So, $\pi_{a,b}$ is a homomorphism of groups.

Let $[x_0 : y_0 : z_0]$ in $E_{a,b}$, then

\[ a = a_0 + a_1 \epsilon + a_2 \epsilon^2 + a_3 \epsilon^3 \]

\[ b = b_0 + b_1 \epsilon + b_2 \epsilon^2 + b_3 \epsilon^3 \]

\[ X = x_0 + x_1 \epsilon + x_2 \epsilon^2 + x_3 \epsilon^3 \]

\[ Y = y_0 + y_1 \epsilon + y_2 \epsilon^2 + y_3 \epsilon^3 \]

\[ Z = z_0 + z_1 \epsilon + z_2 \epsilon^2 + z_3 \epsilon^3 \]

A. Chillali, Department of Mathematic and Computer, FST, Fez, 30000 Morrocco e-mail: (chil2015@yahoo.fr).

Manuscript received Mai 30, 2011
If \([X : Y : Z]\) in \(E_{a,b}\), then
\[
Y^2 Z = X^3 + a X Z^2 + b Z^3.
\]
In order to simplify this last expression, we have
\[
(2) : f_0 + f_1 \epsilon + f_2 \epsilon^2 = 0 + f_3 \epsilon^3 = 0
\]
where
\[
f_0 = -y^2 z_0 + b_0 z_0 + a_0 x_0 z_0^2 + x_0^3,
\]
\[
f_1 = (z_0^2 a_0 + 3 x_0^2) x_1 - 2 y_0 z_0 y_1 + (-y_0^2 + 3 b_0 z_0^2 + 2 a_0 x_0 z_0) z_1 + b_1 z_0 + z_0^3 a_1 x_0,
\]
\[
f_2 = (z_0^2 a_0 + 3 x_0^2) x_2 - 2 y_0 z_0 y_2 + (-y_0^2 + 3 b_0 z_0^2 + 2 a_0 x_0 z_0) z_2 + z_0^2 a_1 x_1 - 2 y_0 z_0 y_1 z_2 - 3 y_2 z_0^2 + 3 x_2 x_0 + 3 b_0 z_0^2 z_2 + b_2 z_0^3 + a_0 x_0^2 z_2 + 2 z_0 z_1 a_1 x_0 + 2 z_0^2 z_1 + 2 z_0^2 a_2 z_0.
\]
\[
(2) \iff f_0 = 0, f_1 = 0, f_2 = 0, f_3 = 0
\]
\[
f_0 = 0 \iff [x_0 : y_0 : z_0] \in E_{\pi(a),\pi(b)}
\]
The coefficients \(z_0^2 a_0 + 3 x_0^2, 2 y_0 z_0 y_1, -y_0^2 + 3 b_0 z_0^2 + 2 a_0 x_0 z_0\) are partial derivative of a function \(F(X, Y, Z) = Y^2 Z - X^3 - a X Z^2 - b Z^3\) at the point \((x_0, y_0, z_0)\), can not be all three null. We can then at last conclude that \([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]\) and \([x_3 : y_3 : z_3]\). Finally, \(\pi_{a,b}\) is a surjective homomorphism of groups.

**Lemma 7:** The mapping
\[
\theta_4 : [\begin{array}{c}
F_3 \\
(l, k, h)
\end{array}] \mapsto [\begin{array}{c}
E_{a,b} \\
[l + k e^2 + h e^3 : 1 : l^3 e^3]
\end{array}]
\]
is a injective homomorphism of groups.

**Proof 8:** Evidently, \(\theta_4\) is injective.

Every \([l + k e^2 + h e^3 : 1 : l^3 e^3]\) satisfies the equation of \((*)\), which calls its points points at infinity of the curve \(E_{a,b}\). We have:
\[
[l + k e^2 + h e^3 : 1 : l^3 e^3] = [l + l' e + k (k+e^2) + h (h + k') e^3 : 1 : (l + l')^3 e^3]
\]
Finally \(\theta_4(l(k, h) + (l', k', h')) = \theta_4(l(k, h) + \theta_4(l', k', h'))\), and we concluded \(\theta_4\) is injective homomorphism of groups.

**Definition 9:** We define \(G_4\) by \(G_4 = \ker(\pi_{a,b})\).

**Proposition 10:** \(G_4 = \theta_4(F_3)\).

**Proof 11:** Let \([l + k e^2 + h e^3 : 1 : l^3 e^3] \in \theta_4(F_3)\), then \(\pi_{a,b}(P) = [0 : 1 : 0]\). Let \(P = [X : Y : Z] \in \ker(\pi_{a,b})\), then \(\pi_{a,b}(P) = [0 : 1 : 0]\).

We set \(X = z_1 \epsilon + x_1 \epsilon^2 + x_1 \epsilon^3, Y = 1 + y_1 \epsilon + y_2 \epsilon^2 + y_3 \epsilon^3, Z = z_1 \epsilon + z_2 \epsilon^2 + z_3 \epsilon^3, Z = z_1 \epsilon + z_2 \epsilon^2 + z_3 \epsilon^3\), and \(Y^{-1} = 1 + s_1 \epsilon + s_2 \epsilon^2 + s_3 \epsilon^3\).

So, \(P = [Y^{-1} X : 1 : Y^{-1} Z] = [z_1 \epsilon + z_2 \epsilon^2 + z_3 \epsilon^3 : 1 : z_1 \epsilon + z_2 \epsilon^2 + z_3 \epsilon^3]\).

We have \(P \in E_{a,b}\), then \(z_1 = 0, z_2 = 0, z_3 = x_1^3\) and \(P \in \theta_4(F_3)\).

Finally, \(G_4 = \theta_4(F_3)\).

**Corollary 12:** The group \(G_4\) is an elementary abelian \(p\)-group, called group at infinity of \(E_{a,b}\).

**Corollary 13:** The sequence
\[
0 \to G_4 \to E_{a,b} \xrightarrow{\pi_{a,b}} E_{\pi(a),\pi(b)} \to 0
\]
be a short exact sequence defining the group extension \(E_{a,b}\) of \(E_{\pi(a),\pi(b)}\) by \(G_4\).

**III. A STRONGLY RESISTANT FUNCTION ON**

Let \(m\) be a prime number such that \(s = \frac{m-1}{2}\) is also prime. Let \(P\) and \(Q\) be two elements of order \(m\). Assume that is difficult to calculate \(r = \log_P Q\). We define the function \(h\) by:
\[
\begin{align*}
0, 1, 2, \ldots, s - 1 & \rightarrow E_{a,b} \\
(x, y) & \rightarrow x P + y Q
\end{align*}
\]

**Theorem 14:** All collision in the function \(h\) allow to calculate \(r\).

**Proof 15:** Suppose we have a collision i.e., there are two distinct pairs \((x, y)\) and \((x', y')\) such as
\[
x P + y Q = x' P + y' Q.
\]
This gives
\[
(x - x')P = (y' - y)Q.
\]
Therefore
\[
(x - x') = r(y' - y)P.
\]
i.e.
\[
(x - x') = r(y' - y)[m].
\]
Let \(d = \gcd(2s, y' - y)\).

Since \(s\) is prime and \(y' - y < s\), then \(d = 1\) or \(d = 2\).

If \(d = 1\) then, we calculate \(z\) the inverse of \(y' - y\) mod \(m - 1\), therefore \(r = (x - x')z[m - 1]\).

If \(d = 2\) then we calculate \(z\) the inverse of \(y' - y\) mod \(s\), therefore \(r = (x - x')z[m - 1]\) or \(r = (x - x')z[s - m - 1]\).

**Remark 16:** The function \(h\) is strongly collision resistant.

**IV. IDENTIFICATION METHODS ON**

Let \(m\) be a prime number such that \(s = \frac{m-1}{2}\) is also prime. Let \(P\) and \(Q\) be two elements of order \(m\). An Authority form a pair \((x_A, y_A)\) from the identity of Alice. It chooses a random number \(0 \leq d \leq m - 1\), computes \(P_A = dh(x_A, y_A)\) and sends it to Alice.

1) Alice chooses a random number \(0 \leq a \leq m - 1\) and compute \(K = aP_A\).
2) Alice sends \(K\) to Bob.
3) Bob chooses a random number \(0 \leq b \leq m - 1\), computes \(B = bh(x_A, y_A)\) and sends it to Alice.
4) Alice computes \(C = ah(x_A, y_A) + aB\) and sends it to Bob.
5) Bob computes \(D = b^{-1}C\) and sends it to authority.
6) The authority calculate \(E = dD\) and sends it to Bob.
7) Bob verifies that \(K = b(E - K)\).

Under this protocol, Bob identifies Alice without disclosure information.
VI. KEY DISTRIBUTION PROTOCOLS

Let \( m \) be a prime number such that \( s = \frac{m-1}{2} \) is also prime. An Authority distributes a random number \( 0 \leq k \leq m-1 \), sends it to Alice and to Bob.

1) Alice take a private key \( t \) such that \( 0 \leq t \leq m-1 \), compute \( P_A = h(t, kt) \), and he transmits \( P_A \) to Bob.

2) Similar, Bob takes a private key \( l \) such that \( 0 \leq l \leq m-1 \), computes \( P_B = h(l, kl) \), and transmits \( P_B \) to Alice.

3) Then Alice and Bob computes \( tP_B \) and \( lP_A \) respectively.

The secret key is \( K = tP_B = lP_A \).

VII. DESCRIPTION OF CRYPTOSYSTEM BASED ON \( E_{a,b} \)

Let \( m \) be a prime number such that \( s = \frac{m-1}{2} \) is also prime. Let \( P \) and \( Q \) be two elements of order \( m \).

1) Space of lights: \( P = E_{a,b} \).

2) Space of quantified: \( C = E_{a,b} \).

3) Space of the keys: \( K = E_{a,b} \).

4) Function of encryption: \( \forall K \in K, e_K : P \rightarrow C \) \( P \rightarrow X+K \)

5) Function of decryption: \( \forall K \in K, d_K : C \rightarrow P \) \( X \rightarrow X-K \)

Remark 17:
\( d_K \circ e_K (X) = X \)

Secret key:
\( K \)

Public keys:
\( \text{Espace of lights } P \)

VIII. CONCLUSION

The conclusion in this work we study the elliptic curve over the artinian principal ideal ring \( A = \mathbb{F}_q[\epsilon], \epsilon^4 = 0 \). More precisely, we establish a group homomorphism between \( (\mathbb{F}_q^*, \times) \) and the abelian group \( E_{a,b} \) of elliptic curve. For cryptography applications, we give a strongly collision resistant function on \( E_{a,b} \) and identification methods on \( E_{a,b} \).

ACKNOWLEDGMENT

I would thank Professor M. E. Charkani and H. Benaza for his helpful comments and suggestions.

REFERENCES